



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,884	05/17/2006	Osamu Aoki	P06,0069	5969
26574	7590	09/26/2008	EXAMINER	
SCHIFF HARDIN, LLP PATENT DEPARTMENT 6600 SEARS TOWER CHICAGO, IL 60606-6473				SHEPELEV, KONSTANTIN
ART UNIT		PAPER NUMBER		
2131				
			MAIL DATE	DELIVERY MODE
			09/26/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/579,884	AOKI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	KONSTANTIN SHEPELEV	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 17 May 2006.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) 1-16 is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 17-32 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>04/16/2007</u> .  | 6) <input type="checkbox"/> Other: _____ .                        |

## **DETAILED ACTION**

This office action is in response to application filed on May 17, 2006 in which claims 17-32 are presented for examination.

### ***Status of Claims***

Claims 1-32 are pending; of which claims 1 and 29-32 are in independent form. Claims 1-16 are canceled. Claims 31 and 32 are rejected under 35 U.S.C. 101. Claims 17, 18, and 27-32 are rejected under 35 U.S.C. 102(e). Claims 19-26 are rejected under 35 U.S.C. 103(a).

### ***Claim Objections***

1. Claim 30 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 29. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

2. Claim 32 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 31. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

***Claim Rejections - 35 USC § 101***

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 31 and 32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 31 recites “an unauthorized-operation-judgment program” which is clearly a functional descriptive material, software, per se. When recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. However, the claim language lacks the necessary computer readable medium, and as such fails to fall within one of four statutory categories of invention according to 35 U.S.C. 101. Therefore, claim 31 is non-statutory.

Claim 32 is rejected in view of the same reasons stated in the rejection of claim 31.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 17, 18, 27-32 are rejected under 35 U.S.C. 102(e) as being anticipated by McCallam et al. (US 2004/0230832 A1).

With respect to claim 17, McCallam teaches the limitation of “an operation-receiver for receiving instruction data for executing said operation” (page 4, paragraph 0047) as the user input manager receives user inputs and directs those inputs to the data analyzer for execution.

In addition, McCallam teaches the limitations of “a first profile-creator for creating a first profile from said instruction data related to the operation for which instruction data was received by said computer”, “a first profile-storer for storing said first profile that was created by said first profile-creator”, “a second profile-creator for identifying a user that executed said operation by said instruction data, and creating a second profile related to the operation executed by said user”, and “a second profile-storer for storing, according to user, said second profiles created by said second profile-creator” (page 6, paragraph 0066) as the detection manager contains software routines, data storage, and processing means to detect an IW attack anywhere on the LAN.

Detection may be based on a number of potential activities that are monitored by the detection manager. For example, insider misuse can be detected when an authorized user performs an unauthorized, or perhaps, infrequent operation that may raise the suspicion that the authorized user's computer is being misused. In another example, user profile data may be stored in a database and may be used to detect an intrusion. The user may have access to a particular database but has not accessed the database for over a year. A sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

Finally, McCallam teaches the limitation of “a score-calculator for comparing said instruction data with at least one profile that is stored in said first profile-storer or in said second profile-storer, and calculating a score for determining whether said operation is an unauthorized operation” (page 6, paragraph 0068) as the comparator may examine data at network devices and compare the data to a predefined condition and (page 6, paragraph 0069) the comparator compares the collected parameters to an established user profile that reflects normal operation of the network device.

With respect to claim 18, McCallam teaches the limitations of “a first log-data-storer for storing log data of said computer”, “a second log-data-storer for storing log data according to a user of said computer”, “wherein said first profile-creator references said first log-data-storer when creating said first profile”, and “wherein said second profile-creator references said second log-data-storer when creating said second profile” (Fig. 5E; page 6, paragraphs 0067 and 0069) as a data storage device 379 containing the user profiles 400 and trend of the performance parameters 410.

With respect to claim 27, McCallam teaches the limitation of “a warning-process for executing a process for displaying a warning on an operation screen of said computer, or generating a warning alarm on said computer, when said score exceeds a reference value” (page 6, paragraph 0066) as a sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

With respect to claim 28, McCallam teaches the limitation of “a warning-notification-transmitter for sending a notification warning to an administration server operated by an administrator of said computer that there is a possibility of an unauthorized operation, when said score exceeds a reference value” (page 6, paragraph 0068) as the comparator may examine data at network devices and compare the data to predefined condition. The detection manager may provide an alert or other means of notifying the security server.

With respect to independent claim 29, it is rejected in view of the reasons stated in the rejection of claim 17.

With respect to independent claim 30, it is rejected in view of the reasons stated in the rejection of independent claim 17.

With respect to independent claim 31, it is rejected in view of the same reasons stated in the rejection of independent claim 17.

With respect to independent claim 32, it is rejected in view of the same reasons stated in the rejection of independent claim 17.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2131

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 19-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over et al. (US 2004/0230832 A1), further referred to as publication 832, in view of McCallam (US 2004/0230834 A1), further referred to as publication 834.

With respect to claims 19-26, it is noted that McCallam does not explicitly teach the limitations of these claims in publication 832.

On the other hand, McCallam teaches the abovementioned limitations in publication 834 as listed below:

With respect to claim 19, publication 834 teaches the limitation of “a login-detector for executing a process for detecting whether a certain user is logged into said computer; wherein when said login-detector detects that a certain user is logged in, said second profile-creator creates a second profile related to said user” (page 4, paragraph 0034) as the database may store the local version of the user profile. The database may also store historical values of the computer performance parameters and the user profile.

With respect to claim 20, publication 834 teaches the limitation of “said login-detector executes detection processing at specified intervals while said computer is in operation” (page 3, paragraph 0032) as the service manager that determines a periodicity of monitoring computers and other network devices for indication of intrusion and misuse.

With respect to claim 21, publication 834 teaches the limitation of “when said login-detector does not detect that a certain user is logged in even though detection processing is executed, said first profile-creator creates a first profile related to said computer” (page 6, paragraph 0056) as the data analyzer sets an initial user profile for a user, where (page 4, paragraph 0035) to create the user profile the data analyzer may invoke an “expected” user profile based on historical usage patterns.

With respect to claim 22, it is rejected in view of the reasons stated in the rejection of claim 20.

With respect to claim 23, publication 834 teaches the limitations of “a third profile-creator for creating a third profile related to an operation executed by a user that is identified as a first-time user, when the user executing said operation by said instruction data is identified as a first-time user operating said computer for the first time”, “a third profile-storer for storing third profiles that are created by said third profile-creator”, and “said score-calculator uses at least one profile that is stored in said third profile-storer instead of said second profile-storer to determine whether said operation is an unauthorized operation” (page 4, paragraph 0035) as the data analyzer may initially create, and then update the user profile. To create the user profile, the data analyzer may invoke an “expected” user profile based on historical usage patterns. This initial user profile can then be quickly updated to match the actual usage patterns of the individual user. Once the user profile is established, the data analyzer reviews long term usage patterns of the individual user, and periodically updates the user pattern.

With respect to claim 24, it is rejected in view of the same reasons as stated in the rejection of claim 23.

With respect to claim 25, publication 834 teaches the limitation of “said score-calculator calculates a score by calculating a deviation between said instruction data and data that is stored in said profiles” (page 4, paragraph 0038) as the comparator compares the computer performance parameters measured by the software agents to the user profile and determines when the comparison warrants taking action.

With respect to claim 26, publication 834 teaches the limitation of “an operation-stopper for executing a process for stopping said operation when said score value exceeds a reference value” (page 6, paragraph 0054) as the messaging manager receives inputs from comparator, and formulates and forwards status and action messages to other components. The associated action message may automatically direct the execution of this action.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of publication 834 into the system described in the publication 832 to provide a more efficient method for detecting misuse at each individual computer in a network.

***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:
- a. Zare et al. (US 2006/0010258 A1).
  - b. Tono et al. (JP2002-132800A).
  - c. Kobayashi (JP2001-092783A).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 8:30 - 18:00, Fri 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/  
Examiner, Art Unit 2131

9/24/2008

/Syed Zia/  
Primary Examiner, Art Unit 2131